DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 0226289.7 (UNITED KINGDOM) , filed on 11/11/2002.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 11/22/05, 05/29/08 was filed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

3. Figures 1-2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to because of the following informalities: The acronym " CN (CNAddr), GGSN, IPN, MN (CoA), MN (HAddr), HA, PD , T2H, PCD " need to be spelled out. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities: The claim 20 contains subject matter "A computer readable medium including a program for executing a method" which was not described in the specification.

Appropriate correction is required.

6. Claims 1-11, 12-14, 15, 16-18, 19, 20, 21 are presented for examination

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless —
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-2, 12-13, 15, 21 are rejected under 35 U.S.C. 102(e) as being anticipated by O'neill (Pub No.: US 2004/0100951 Al).

Regarding to claim 1, O'neill discloses the a method of filtering (figure 13, trigger events) data packet at a network gateway (figure 11, Router node 200), comprising:

♦ the data packets having a header including a destination address (figure 4, CN address) and an extension header (figure 4, Option field 38 includes CoA "care of address"), the method comprising selectively blocking (figure 13, discard packet 480) ones of the data packets wherein neither the destination address (figure 13, destination header) nor the extension header matches a predetermined address criterion (figure 13, step 410, monitor for IP packets that match a trigger event) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and using destination header) (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph [0156] following the decision to either forward or discard the packet as a result of triggers 416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step 490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events).

Regarding to claim 2, O'neill discloses wherein the address criterion (figure 13, the router node includes trigger event to filter the IP packets) is applied only to packet transmitted from a source node (figure 3, mobile node) to a destination node (CN node) during a corresponding packet data communication session (page 4 paragraph [0059] Session: A communication relationship that typically involves a bi-directional flow of packets between a mobile node and at least one corresponding node).

Regarding to claim 12, O'neill discloses the a method of filtering (figure 13, trigger events) data packet at a network gateway (figure 11, Router node 200), comprising:

- ♦ the data packets having a header including a destination address (figure 4, CN address), the method comprising selectively blocking (figure 13, discard packet 480) ones of the data packets where the destination address (figure 13, destination header) does not meet a destination address criterion (figure 13, step 410, monitor for IP packets that match a trigger event) which defines an address (destination header) of at least one forwarding agent which forward packets addressed to the forwarding agent to a destination node (corresponding node) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and using destination header) (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph [0156] following the decision to either forward or discard the packet as a result of triggers

416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step 490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events).

It is alternative conditions (where the destination address does not meet 1) a destination address criterion or 2) a forwarding agent criterion which defines an address of at least one forwarding agent which forwards packets addressed to the forwarding agent to a destination node at a network address specified in the payload of the packet). The examiner applied the prior art rejection on wherein the destination address does not meet a destination address criterion.

Regarding to claim 13, O'neill discloses wherein the at least one forwarding agent (figure 3, page 5, [0065] the FAR 54, HAR 59, and HA 58 are at least option enforcement points) blocks packets for which the network address (destination header) does not meet the destination criterion (figure 13, step 410, trigger event) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and using destination header) (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph [0156] following the decision to either forward or discard the packet as a result of triggers 416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step 490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events).

Regarding to claim 15, O'neill discloses a method of transmitting data packets in a source node (figure 8, correspondent node 82), comprising:

- Establishing a packet data communication session with a destination node (figure 8, mobile node 72) at a first network address (home address) via a network gateway (figure 8, FAR 74, OEP 76 "Option enforcement point") such that the gateway applies a filter to the data packets of the communication session based on a destination address (destination header) of the data packet (figure 13, step 410, trigger event) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and using destination header) (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph

[0156] following the decision to either forward or discard the packet as a result of triggers 416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step 490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events);

- Receiving an indication of a second network address of the destination node (mobile node) during the session (the mobile node informs the correspondent node its care-of address) (page 3 paragraph [0019] the MN can be reasonably confident that the CN knows the desired binding between the MN HoA and the MN CCoA. The CAO, while being well suited for unicast communications, may also be used to enable the HoA to be used as a multicast source address on a foreign subnet thereby allowing packets constructed with the HoA as a source address to pass multicast RPF checks which was not possible when the prior art Home Address option, which used the CoA as the source address, was used);
- And transmitting subsequent packet within the session addressed to the second network address (care-of address "CoA") and containing the first address (home address "HoA") in an extension header (figure 2, option field) for containing information to be read by intermediate nodes (figure 8, FAR 74, OEP 76) between the source node (figure 8, correspondent node) and the destination node (figure 8, mobile node 72) (figure 1 paragraph [0006] the header 25 includes a source address 22, a destination address 24, a home address option field 28 includes HoA

"home address").

Regarding to claim 21, O'neill discloses the an apparatus configured to filter (figure 13, trigger events) data packet at a network gateway (figure 11, Router node 200), comprising:

the data packets having a header including a destination address (figure 4, CN address) and an extension header (figure 4, Option field 38 includes CoA "care of address"), wherein the apparatus is configured selectively blocking (figure 13, discard packet 480) ones of the data packets wherein neither the destination address (figure 13, destination header) nor the extension header matches a predetermined address criterion (figure 13, step 410, monitor for IP packets that match a trigger event) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and using destination header) (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph [0156] following the decision to either forward or discard the packet as a result of triggers 416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step

490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 16, 18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'neill (Patent No.: US 2004/0100951 Al) in view of Patil et al. (Patent No.: US 6,973,086 B2).

Regarding to claim 16, O'neill discloses the a method of applying a destination address (figure 13, step 417, destination header) based filtering (figure 13, trigger events) at a network gateway (figure 11, Router node 200) to packet data session between a source node (figure 8, correspondent node 82) and a destination node (figure 8, mobile node 72); comprising:

- ♦ Wherein the destination node (mobile node 72) roams from a home address (HA) in a home network to a care-of address in a foreign network (page 2 [0017], page 3 [0034], the mobile node roams from a home network to foreign network);
- ♦ Sending a binding update to the source node (figure 8, correspondent

node 82) so that the source node (figure 8, correspondent node 82) addresses subsequent packets in the session to the care-of address (page 3 paragraph [0019] the MN can be reasonably confident that the CN knows the desired binding between the MN HoA and the MN CCoA. The CAO, while being well suited for unicast communications, may also be used to enable the HoA to be used as a multicast source address on a foreign subnet thereby allowing packets constructed with the HoA as a source address to pass multicast RPF checks which was not possible when the prior art Home Address option, which used the CoA as the source address, was used);

- Places the home address in an extension header of the subsequent packet (figure 2, home address (HoA) in an extension header of the subsequent packets.

However, O'neill is silent to disclosing the method comprising applying the destination address-based packet filter to the extension header of the subsequent packets.

Patil et al. disclose the home address in an extension header (col. 1, line 59, home address destination option); the method comprising:

Applying the destination address-based packet filter to the extension header of the subsequent packets (applying the filter to the extension header means to applying the filter of home IP address because the extension includes the home IP address) (col. 10, lines 10-15, when the Mobile Node subsequently sends other types of data / messages whose packets include the home address destination option to a Node over the visited networks. The Access Router will determine if the Mobile Node's care of address and / or home IP address is included in the ingress filter and / or an access control list. If true, the packets are forwarded by the Access Router towards its destination) (col. 9, lines 55-67, The Home Agent determines if the included home IP address for the Mobile Node is authentic and/or authorized. If not, the Home Agent does not reply to the binding update message. However, when the home IP address included in the binding update message from the Mobile Node can be authenticated/authorized, the Home Agent sends a binding acknowledgement message to the Mobile Node that includes the home address destination option.....When the Access Router receives the binding acknowledgement message from the Home Agent, it verifies the validity of the home IP address by examining a certificate/security token included in the message. The Access Router also compares the binding acknowledgement message to the state of a previously forwarded binding update message from the Mobile Node. If there is an affirmative match and the home IP address is verifiable, the Access Router adds the Mobile Node's home IP address to its ingress filter and/or access control list).

Both O'neill and Patil disclose filtering the data packets. Patil recognizes Applying the destination address-based packet filter to the extension header of the subsequent packets. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate applying the destination address-based packet filter to the extension header of the subsequent packets taught by Patil into the system of O'neill in order to secure mobile IP home addresses with the mobile IPv6 protocol (see Patil, col. 1, line 15).

Regarding to claim 18, O'neill discloses wherein the extension header (figure 2, option field 28 includes HoA) is read by intermediate nodes (figure 8, FAR 74, OEP 76) between the source node (figure 8, CN node 82) and the destination node (figure 8, mobile node "MN" 72).

Regarding to claim 20, O'neill discloses the a method of filtering (figure 13, trigger events) data packet at a network gateway (figure 11, Router node 200), comprising:

- ♦ the data packets having a header including a destination address (figure 4, CN address) and an extension header (figure 4, Option field 38 includes CoA "care of address"), the method comprising selectively blocking (figure 13, discard packet 480) ones of the data packets wherein neither <u>the destination address</u> (figure 13, destination header) nor the extension header matches a predetermined address criterion (figure 13, step 410, monitor for IP packets that match a trigger event) (figure 13, step 417, No CaO packet, or CoA in destination header so not inspected by Router due to IPv6, header processing rules (e.g. MN home and <u>using destination header)</u> (page 13, paragraph [0153] the processing pass to step 450 where it is determined whether this node 200 has ingress filtering on the source address disabled. If it is disabled the packet is forwarded normally at step 485 whereas if it is not disable then the source address of the packet is once again checked against the unicast or multicast routing table in step 455 to check that the incoming interface is correct and that therefore the source is topologically ok) (page 3 paragraph [0156] following the decision to either forward or discard the packet as a result of triggers 416, 417, 418, 419, the processing passes from either step 480 "discard the packets" or step 485 "forwarding the packets" to step 490 where the subroutine 223 processing for this packet finishes and we return to 410 to monitor packets for trigger events).

O'neill discloses computer readable medium (page 15, claim 13, readable-medium); However, O'neill is silent to disclosing a computer readable medium including a program for executing a method.

Patil et al. disclose a computer readable medium including a program for executing a method (co1.13, lines 6-7, A computer-readable medium that includes instructions for performing actions, including: (a) providing a care of address to a mobile node that employs an access router to communicate with at least one resource over a visited network).

Both O'neill and Patil disclose filtering the data packets. Patil recognizes a computer readable medium including a program for executing a method. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a computer readable medium including a program for executing a method taught by Patil into the system of O'neill in order to secure mobile IP home addresses with the mobile IPv6 protocol (see Patil, col. 1, line 15).

Allowable Subject Matter

17. Claims 3-6, 10-11, 7-9, 14, 17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

18. The following is a statement of reasons for the indication of allowable subject matter:

Claim 3 is objected. O'neill (2004/0100951 Al) discloses wherein the destination node (mobile node) has a first network address (home address) during a first period of the packet data communication session (a mobile node has home address when it is within its home network) and a second, different network address (care-of address) during a second, subsequent period of the data communication session (the mobile node has the care-of address while it is away from home network to foreign network) (page 2 paragraph [0017] [0034] a mobile node roams from home network to foreign network); comprising: The packet include a source address (figure 1, source address), and the source node (correspondent node) transmits packets having the first network address (home address of mobile node as the destination node), during the first period (when it is within its home network), (figure 1, destination address 14 is home of address of the mobile node) (page 1 paragraph [0003] example of the data packets includes a source (S) address 12 and a destination address 14) (page 1, paragraph [0004] a mobile node is often associated with a home network wherein it uses a Home Address (HoA). When visiting a foreign subnet having different address prefix from the

home network, the Mobile Node may be assigned a Care-of address which has the correct address prefix for the visited foreign subnet).
The prior art however fails to disclose transmits packets having the second network address as the destination address and the first network address in the extension header during the second period.

Claim 7 is objected. O'neill (2004/0100951 Al) discloses wherein the source node (mobile node) has a first network address (home address) during a first period of the packet data communication session (a mobile node has home address when it is within its home network) and a second, different network address (care-of address) during a second, subsequent period of the data communication session (the mobile node has the care-of address while it is away from home network to foreign network) (page 2 paragraph [0017] [0034] a mobile node roams from home network to foreign network); comprising: The packet include a source address (figure 1, source address), and the source node (mobile node) transmits, during the first period (when it is within its home network), packets having the first network address (figure 1, source address 12 is home of address of the mobile node) and the destination address of the destination node as the destination address (figure 1, destination addressl4) (page 1 paragraph [0003] example of the data packets includes a source (S) address 12 and a destination address 14) (page 1, paragraph [0004] a mobile node is often associated with a home network wherein it uses a Home Address (HoA). When visiting a foreign subnet having different address prefix from the home network, the Mobile Node may be assigned a Care-of address which has the correct address prefix for the visited foreign subnet); Transmits, during the second period (when visiting the foreign network), packet having the second network address as the source address (see figure 2, CoA is source address).

The prior art however fails to disclosing the address of the destination node in the extension header and, as the destination address, the address of forwarding agent which forwards the packets to the destination node

Claim 14 is objected. The prior art (6973086) discloses a method of filtering (col. 10, lines 9-13, ingress filter) data packets at a network gateway (col. 10, lines 9-13, access router) the data packets having a header including a destination address and an extension header (see col. 5, line 9, home-address destination option); comprising: selectively blocking ones of the data packets where neither the destination address nor the extension header (col. 5, line 5 home-address destination option) matches a predetermined address criterion (col. 10, line 13, Mobile Node's care of address and / or home IP address) (col. 10, lines 10-15, when the Mobile Node subsequently sends other types of data / messages whose packets include the home address destination option to a Node over the visited networks. The Access Router will determine if the Mobile Node's care of address and / or home IP address is included in the ingress filter and / or an access control list. If true, the packets are forwarded by the Access Router towards its destination).

The prior art however fails to disclose wherein the forwarding agent criterion is variable so as to include or exclude an address of the at least one forwarding agent.

Claim 17 is objected. The prior art (6973086) discloses a method of filtering (col. 10, lines 9-13, ingress filter) data packets at a network gateway (col. 10, lines 9-13, access router) the data packets having a header including a destination address and an extension header (see col. 5, line 9, home-address destination option); comprising: selectively blocking ones of the data packets where neither the destination address nor the extension header (col. 5, line 5 home-address destination option) matches a predetermined address criterion (col. 10, line 13, Mobile Node's care of address and / or home IP address) (col. 10, lines 10-15, when the Mobile Node subsequently sends other types of data / messages whose packets include the home address destination option to a Node over the visited networks. The Access Router will determine if the Mobile Node's care of address and / or home IP address is included in the ingress filter and / or an access control list. If true, the packets are forwarded by the Access Router towards its destination).

The prior art however fails to disclose wherein the extension header is used by the destination node to restore the home address as the destination address of the subsequent packets.

22. Claim 19 is allowed.

The following is a statement of reasons for the indication of allowable subject matter: Claim 19 is allowed. Patil discloses a method of applying a destination based filter (ingress filter) at a network gateway (col. 10, lines 10-15, access router) between the source node and a destination node (col. 10, lines 10-15, when the Mobile Node

subsequently sends other types of data / messages whose packets include the home address destination option to a Node over the visited networks. The Access Router will determine if the Mobile Node's care of address and / or home IP address is included in the ingress filter and / or an access control list. If true, the packets are forwarded by the Access Router towards its destination) (col. 9, lines 55-67, The Home Agent determines if the included home IP address for the Mobile Node is authentic and/or authorized. If not, the Home Agent does not reply to the binding update message. However, when the home IP address included in the binding update message from the Mobile Node can be authenticated/authorized, the Home Agent sends a binding acknowledgement message to the Mobile Node that includes the home address destination option when the Access Router receives the binding acknowledgement message from the Home Agent, it verifies the validity of the home IP address by examining a certificate/security token included in the message. The Access Router also compares the binding acknowledgement message to the state of a previously forwarded binding update message from the Mobile Node. If there is an affirmative match and the home IP address is verifiable, the Access Router adds the Mobile Node's home IP address to its ingress filter and/or access control list) (col. 1, lines 40-41 when the packet is received by a CN or HA, they swap the COA in the source address with MN's home address in the payload of each packet); comprising:

Wherein the source node (mobile node) roams from a home address in a home network to a care-of address in a foreign network (visited network having a network gateway (access router), (col. 1, lines 60-63, A care of address is provided to a mobile node that employs an access router to communicate with at least one resource over a visited network. A binding update message from the mobile node is forwarded by the access router to another node for authentication. The other node responds with a binding acknowledgement message to the mobile node if a home IP address included in the binding update message is authentic. If the binding acknowledgement message from the other node is determined by the access router to verify the home IP address for the mobile node, the mobile node can communicate another type of data through the access router with at least one resource over the visited network) (col. 4, lines 6-7, the term "Care-of Address" refers to the termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home) (col. 5, lines 37, when a mobile node first connects to an access point (router) on a visiting network, it obtains a new care-of-address (COA) and sends a binding update message to the HA on its home network or a CN. The access router (first hop router/default router) on the visited network allows this message from the MN to be forwarded, which includes the home-address destination option, because it is a binding update message); And the network gateway applies the destination address filter to the extension header (Home-address destination option includes the home address) of the packet (col. 10, lines 10-15, when the Mobile Node subsequently sends other types of data / messages whose packets include the home address destination option to a Node over the visited networks. The Access Router will determine if the Mobile Node's care of address and / or home IP address is included in the ingress filter and / or an access control list. If true, the packets are forwarded by the Access Router towards its destination).

O'neill discloses setting up a reverse tunnel to home agent in the home network for forwarding packets to the destination node (page 3, paragraph [0018] the Destinaiton Header based CoA (Care-of address) can in addition be used to inform the CN (destination node) of the location of MN when either reverse tunneling to the HA or on the Home network). O'neill discloses the network gateway applies the destination address filter (filter) to the extension header of the packets (the home IP address in an extension header)

The prior art however fails to disclose the source node places the address of the destination node in an extension header of packets sent from the foreign network

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Leung (Patent No.: US 6,636,498 B1); Yano et al. (Patent No.: US 7123599); Grech (Pub. No.: US 2004/0071120 Al).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHUONG T. HO whose telephone number is (571)272- 3133. The examiner can normally be reached on 8:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, EDAN ORGAD can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

/CHUONG T HO/ Temporary Grant of Partial Signatory Authority

Examiner, Art Unit 2619 06/07/08